From: Susan Orr Consulting, Ltd.
To: PRAINFO
Subject: Comments on FFIEC Cyber Assessment Tool
Date: Monday, September 14, 2015 5:47:51 PM
Attachments: PastedGraphic-1.pdf

In working with several banks on completing the assessment tool several questions have come up:

Part 1:
1. There is nothing that really explains how to tie Part 1 and Part 2 together.
2. Global remittances - most community banks don't know if they do global remittances or not and there isn't a really clear definition available on the Internet. Would be beneficial to provide a definition: what are/constitutes a global remittance. Even asked an examiner and they didn't know.
3. Treasury services - do you mean online cash management (online origination of ACH and/or WT) by customers)?

Part 2:
Domain 1: Cyber Risk Management and Oversight
IT Asset Management
1. Evolving statement: Can you define: asset life-cycle process? What would that look like?

Domain 3: Cybersecurity Controls
Infrastructure Management
1. Evolving statement: Domain Name System Security (DNSSEC) is deployed. Most community banks have no clue what DNSSEC is, and most IT professionals state that they do not deploy this across the network. Does this statement need to be in Evolving or could it be moved to Advanced? Seems more like an Advanced control.

Secure Coding
1. Baseline statements 1 &2; Intermediate and Advanced Statements - most community banks do not do any coding but only a few statements note to answer NA if don't do software development. Why don't you make this a section that is NA unless a bank has developers and does programming and coding?

Remediation
1. Intermediate statement 2: Repeat pen testing to confirm vulnerabilities resolved…I know of no community bank that will pay to have another pen test after remediation has been implemented. Very difficult to get some banks to have one annually let alone have another one right after they just had one. I agree that is a good thing to do but not a reality. Therefore most banks will not ever move beyond Evolving.

Domain 4: External Dependency Management
Due Diligence
1. Intermediate statement 2: pre-contract onsite visits, I can't imagine any size bank is going to do this. There is also currently nothing that mandates it is done. Wouldn't it make more sense to have this in an Advanced or Innovative statement? Most banks are not going to move beyond Intermediate due to this statement.

Domain 5: Cyber Incident Management

Planning

1. Intermediate statement 3: not that it isn't a great idea but most community banks are not going to be able to afford the luxury of having a "contract" in place or pay a retainer to have a forensic specialist/company on the ready if something were to happen. They are at least starting to do the research and identify firms and have a contact in case they need it and some even get an idea of the cost involved (hourly fee). Some are starting to use the US Secret Service as an initial contact and have their forensic people help them. Would this constitute a yes answer to this question? Otherwise like several other statements, the bank will not move past Evolving.

Thank you.

Regards,
Susan
CISA, CISM, CRISC, CRP

Susan Orr Consulting, Ltd.
2863 W. 95th Street
Ste. 143 #223
Naperville, IL 60564
630.499.0276 Office
630.248.7788 Mobile
www.susanorrconsulting.com
https://securecontact.me/susan@susanorrconsulting.com